



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,350	11/17/2000	David Montgomery	0500.0003231	6328

23418 7590 07/14/2005

VEDDER PRICE KAUFMAN & KAMMHOLZ  
222 N. LASALLE STREET  
CHICAGO, IL 60601

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT PAPER NUMBER

2134

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/715,350

Applicant(s)

MONTGOMERY, DAVID

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 15 April 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-7, 12-17, 19-21, 24-33, 35 and 37-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 2, 4-7, 12-17, 19-21, 24-33, 35, 37, 38, 40, 41, 43, 45 and 46 is/are rejected.
- 7) ☒ Claim(s) 3 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 4/15/05.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. The response of 4/15/2005 was received and considered.
2. Claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46 are pending.

### ***Response to Arguments***

3. In light of Applicant's amendments to the claims and response (p. 14), the rejection of claims 1-7 and 12-15 under 35 U.S.C. §101, set forth in the previous Office Action, is withdrawn.
4. In the previous Office Action, a rejection under 35 U.S.C. §112 ¶2 was made indicating that the term "signed certificate set" can be interpreted as equivalent to "a set of certificates that is signed" or to "a set of signed certificates", rendering the claim indefinite. Applicant argues the following:

"the term "signed certificate set" is not limited to a set of certificates that is signed, such as a plurality of cross certificates, but may include the public keys thereof or information sufficient to retrieve the public keys in a secure way or the associated public key of a cross certificate, or reference to the public key, or any other suitable cross certificate data. However, this set of certificate related data is signed. (See for example, specification, page 12, line 28 through page 13, line 22 and elsewhere.) In addition, the public key of each trusted certificate issuing unit may be the public key itself or an indirect link to the public key or any suitable representation thereof (see for example, page 11, lines 14-17). In addition, the term signed certificate sets as set forth in the specification does not include just a set of signed certificates as alleged in the office action. As set forth, for example, in claim 1 the signed certificate sets include at least a unique identifier and the public key of each trusted certificate issuing unit as the term public key as used in the specification."

The specification gives the following description for the term "signed certificate set":

- a. It may contain a list of CAs, trusted by trust anchor certificate issuing unit" (p. 12, lines 17-18);

Art Unit: 2134

- b. It may contain no entries (p. 12, lines 18-19);
  - c. It may contain a list of unique CA identifiers and associated public keys of each certificate issuing unit trusted by the anchor certificate issuing unit (p. 12, lines 22-26);
  - d. It may contain a data from the certificate or the certificate itself, along with a unique identifier and its associated public key (or reference to the public key, for example a secure hash of the public key) (p. 12, line 28 – p. 13, line 2).
  - e. It may contain a sequence of cross certificates and/or just the public keys (or information sufficient to retrieve the public keys in a secure way, for example the public key identifier and a secure hash of the public key) of the trusted certificate issuing units determined to be valid via cross certification relationships” (p. 13, lines 18-24); and
  - f. It may be signed (p. 15, lines 14-15).
5. Given the above descriptions in the specifications, the limitation “signed certificate set” in the claims may contain nothing, a list of identifiers and public keys, certificates, references to public keys, or some combination thereof and that the signed certificate set may be signed. Therefore, “signed certificate set” will only be limited by what is included in the signed certificate set according to the claim language and no patentable weight is given to the term “signed”. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, the rejections of claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46 under 35 U.S.C. §112 ¶2 are maintained. Further, Applicant's response (p. 15, ¶2 & p. 17, ¶1) relating to the “inconsistency of the interpretation made in the previous Office Action is not persuasive.

Art Unit: 2134

6. Applicant's response (p. 16, ¶2-3) is persuasive.
7. Applicant's response (p. 16, ¶4) argues that there does not appear to be any teaching or suggestion of a signed certificate set which contains information relating to multiple trusted certificate issuing units. Regarding Applicant's response to the rejection of claims 2 & 27, while it is understood that the user's keyring is meant to contain a plurality of signed public keys, the reference fails to disclose explicitly a plurality rather than a single public key and therefore this argument is persuasive. This argument, however, does not apply to claim 31, as the claim does not require a plurality of certificate issuing units.
8. Applicant's response (p. 17, ¶1) argues that NAI fails to disclose the subject matter of claim 3, wherein the method includes a step to collect one of a plurality of cross certificates by obtaining chained cross certificates and creating a signed set therefrom. This argument is persuasive.
9. The arguments above are persuasive and therefore, the rejections based on the NAI reference are withdrawn. However, an updated search has revealed new art pertinent to the claimed subject matter. In application of this newly cited art, this action is made non-final.

#### ***Claim Objections***

10. Claim 1 is objected to because of the following informalities: "trusted certificate issuing unit" (last line) should be replaced with "trusted certificate issuing units". Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 112***

Art Unit: 2134

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46, "signed certificate set" can be interpreted as equivalent to "a set of certificates that is signed" or "a set of signed certificates" and the claims are therefore vague and indefinite.

Regarding claim 15, the limitation "when identifying trusted certificate issuing unit certificates" has no clear antecedent basis.

### ***Claim Rejections - 35 USC § 101***

13. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 16-17, 19-21, 24-29, 38-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to subject matter not necessarily carried out using a computer or an apparatus containing software, per se. A claim preamble containing "computer system" rather than "system" will overcome this rejection.

### ***Claim Rejections - 35 USC § 103***

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 1-2, 4-7, 12-17, 19-21, 24-33, 35, 37-38, 40-41, 43 & 45-46, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,304,974 to Samar, in view of Menezes.

Regarding claims 1, 4, 6-7, 12, 14, 16, 19-21, 24, 26, 29-30, 32-33, 35, 41 & 46, Samar discloses for a community of interest, collecting at least one cross certificate/list of certificates (col. 6, lines 14-21) associated with another anchor certificate issuing unit/enterprise administrator, and obtaining at least one certificate issuing unit/ trusted certificate authority (col. 6, lines 14-21) public key and associated identifier for a cross-certified certificate issuing unit/trusted certificate authority identified by the at least one cross certificate (col. 6, lines 28-34) and creating a signed certificate set (col. 6, lines 28-34) identifying a plurality of certificate issuing units/certificate authorities determined to be trusted by the anchor certificate issuing unit/enterprise administrator based on the at least one cross certificate/list of certificates, wherein the signed certificate set includes at least the unique identifier and the public key (certificate) of each of the plurality of trusted certificate issuing units (col. 6, line 24 – col. 7, line 16). Samar lacks explicitly collecting cross certificates in creating the signed certificate set. However, Menezes teaches that a cross-certificate is a certificate created by one certification authority to certify the public key of another (p. 572, 13.39 Definition). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify

Art Unit: 2134

Samar to collect the enterprise administrator's cross-certificates to build the list of trusted CA's.

One of ordinary skill in the art would have been motivated to perform such a modification because a cross-certificate is a certificate created by one certification authority to certify the public key of another, as taught by Menezes (p. 572, 13.39 Definition).

Regarding claims 2, 17, 27-28 & 31, Samar lacks generating a signed certificate set revocation list. However, Menezes teaches that a certificate revocation list is a signed list of revoked public keys (certificates), including an identifier of the associated certificate (p. 577) when a CA loses trust in a particular public key (p. 576, §13.6.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a signed certificate set revocation list containing at least an identifier of at least one signed certificate set that has been revoked. One of ordinary skill in the art would have been motivated to perform such a modification to prevent subsequent use of or trust in a certificate, as taught by Menezes (pp. 576-577).

Regarding claims 5 & 37, Samar lacks explicitly requests by one or more clients. However, the examiner takes Official Notice that a client requesting a service is old and well established in the art of the user/administrator model as a method of servicing a client through an administrator. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Samar's enterprise administrator to further accept request from a client for the certificate list. One of ordinary skill in the art would have been motivated to perform such a modification to service a client's need for a certificate list. This advantage is well known to those skilled in the art.



Regarding claims 13 & 25, Samar, as modified above, discloses identifying trusted certificate issuing units based on cross certificates and conveying that trust to clients, but lacks explicitly validating a digital signature associated with each cross certificate and only including certificate issuing units that had valid certificates. However, Menezes teaches that the purpose of certificates are to be validated to determine authenticity of a public key (p. 560, §13.23 (ii)) and to convey trust in that public key to another entity (definition 13.22). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to validate the digital signature on the trusted CA's certificates and only include valid certificates in the signed certificate set/list of trusted certificates. One of ordinary skill in the art would have been motivated to perform such a modification to only convey trust in valid certificates, as taught by Menezes (pp. 559-560).

Regarding claims 15, 38, 43 & 45, Samar lacks including identifiers of policy constraints in the signed certificate set. However, Menezes teaches that including expiration dates in certificates limits exposure following compromise (p. 577, #1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the certificate list of Samar to include a policy identifier/expiration date. One of ordinary skill in the art would have been motivated to perform such a modification to limit exposure following compromise, as taught by Menezes (p. 577, #1).

Regarding claim 40, Samar lacks adding assigned certificate set identifier associated with a given anchor certificate issuing unit. However, Menezes teaches that common forms of additional information are added to certificates, such as a serial number to identify the certificate (§13.4.2). Therefore, it would have been obvious to one having ordinary skill in the art at the

Art Unit: 2134

time the invention was made to include a serial number in the signed certificate set. One of ordinary skill in the art would have been motivated to perform such a modification to identify the certificate set, as taught by Menezes (§13.4.2).

***Allowable Subject Matter***

17. Claim 3 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

(703)746-7239 (after July 15, 2005 use **571-273-8300**) (for formal communications intended for entry)

**Or:**

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")


Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS  
June 27, 2005



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100